Regarding (a), under MPEP 2173.02 it is required that claims ". . . define the patentable subject matter with a <u>reasonable</u> degree of particularity and distinctness." (Emphasis in the original.) MPEP 2173.02 states: "If upon review of a claim **in its entirety**, the examiner concludes that a rejection under 35 U.S.C. 112, second paragraph, is appropriate, such a rejection should be made and an **analysis** as to why the phrase(s) used in the claim is 'vague and indefinite' should be included in the Office Action." (Emphasis added.) Neither of these criteria has been met by the Examiner's assertion: *"The claims each contain the phrase: 'substantially simultaneously"* [sic] *It is not clear what is meant by 'substantially' in this context."* This is a conclusory statement with no analysis of why the phrase is considered by the Examiner to be "vague and indefinite" in the context of the claim considered as a whole, so that a prima facie case of indefiniteness has not been established. The phrase "substantially simultaneously" appears to have been considered on a stand alone basis instead of in the context of the rejected claim considered as a whole, particularly noting that all the rejected claims require the recited "exponentiation operations" be carried out as part of primality testing operations performed "in parallel" <u>and</u> "substantially simultaneously". "Substantially" modifies "simultaneously" which itself is definite and is associated with "in parallel" which also is definite. The phrase "substantially simultaneously" avoids implication that those claims necessarily required parallel performance of the recited "exponentiation operations" in exact coincidence. This is emphasized by the statement at page 10, lines 8-9, "The present invention provides a system and method for efficient parallel prime number searching." Each of the rejected claims considered as a whole would have apprised a person of ordinary skill in the relatively sophisticated art of cryptographic systems, at the time of the invention, aware that characteristics may differ between prime number candidates being tested, of the scope of the claim. The Federal Circuit has stated that "[c]laims need only 'reasonably apprise those skilled in the art' as to their scope to satisfy the definiteness requirement. . . . In addition, the use of modifiers in the claim, like 'generally' and 'substantial,' does not by itself render the claims indefinite." Energy Absorption Sys., Inc. v. Roadway Safety Servs., Inc., Civ. App. 96-1264 (Fed. Cir. July 3, 1997) (unpublished). Consequently, the notice function required by 35 U.S.C. 112, second paragraph is served – see MPEP 2173.02. Withdrawal of this rejection is respectfully requested.

Independent claim 15 and its dependent claims 17 and 20; independent claim 24 and its dependent claim 27; independent claim 36 and its dependent claims 37, 39 and 41; independent claim 45 and its dependent claims 47 and 49; and independent claim 53 all were rejected only under 35 US 112,

second paragraph, and not on the basis of prior art. Consequently all of those claims should be in condition for allowance. In addition, none of claims 16, 18, 19, 21-23 (dependent directly or indirectly from claim 15); 25, 26 (dependent directly or indirectly from claim 24); claims 38, 40, 42-44 (dependent directly or indirectly from claim 36); 46, 48 and 50-52 (dependent directly or indirectly from claim 45), also should be in condition for allowance together with their parent claims.

<u>Claim Rejections under 35 USC 103</u>

Claims 1, 12, 13, 14, 28, 29, 31, 32, 34, 54 and 57 were rejected under 35 US 103 as allegedly obvious over Handbook of Applied Cryptography, Menezes et al., CRC Press 1996, pages 134-168 (Menezes) in view of Quisquater et al., *"Fast Decipherment Algorithm for RSA Public Key Cryptosystem"*, Oct. 1982, Electronic Letters, Vol. 19, No. 21 (Quisquater).

In rejecting claim 1, the Examiner asserts in Section 5 of the Office Action:

> *". . . Menezes teaches a process of searching for a plurality of prime number values, comprising the steps of: randomly generating a plurality of k random odd numbers each providing a prime number candidate (Sec. 4.1.1, p. 134); and performing at least one primality test on each of said candidates (Sec. 4.1.1, p. 134), each of said primality tests including an associated exponentiation operation (Sec. 4.2.3 p. 138-140)."*

This assertion is respectfully traversed. At Sec. 4.1.1, Menezes discusses generation of large prime numbers using an approach:

> "1. Generate as *candidate* a random odd number *n* of appropriate size.
> 2. Test *n* for primality.
> 3. If *n* is composite, return to the first step."

That is, a candidate (singular) is generated and primality testing is carried out that candidate. Candidates are selected and tested <u>one</u> candidate at a time in a sequential manner – see step 3 above. Menezes does not disclose or suggest what is claimed in claim 1:

> "randomly generating a plurality of k random odd numbers each providing a prime number candidate; and performing a plurality of t primality tests on each of said plurality k of randomly generated prime number candidates, each of the plurality of **(k x t)** primality tests . . . executed by an associated one of a plurality of **(k x t)** of the exponentiation units, said exponentiation operations being performed in parallel . . .."

The Examiner does concede, properly:

> *"Menezes does not teach a processing system including a processing system including a processing unit and a plurality of exponentiation units communicatively coupled to the*

> *processing unit, or that the primality tests are carried out by the plurality of exponentiation units in parallel . . ."*

In rejecting claim 28, the Examiner asserts in Section 5 of the Office Action:

> *"As for claim 28, Menezes teaches a prime number generating process of searching in parallel for a plurality of prime number values, comprising the steps of randomly generating a plurality of k random odd numbers expressed as no,o, n1,o, . n((k-1)),0,* [sic] *each said number providing a prime number candidate; determining a plurality of y additional numbers based on each one of the randomly generated odd numbers no,o, n1,o, n(k-1),O* [sic] *to provide kXy) additional prime number candidates (no,,, 110,2, no,y), (n1,1, n1,2, n1,y), . (n(k-1),1, n(k-1),2, n(k-1);,)* [sic] *thereby yielding a total number of (k r (y+1))* [sic] *prime number candidates (Page 148, Sec.4.5.1)* [sic - Sec. 4.51] *sieving said (k x (y+1) prime number candidates by performing a small divisor test on each of said candidates in order to eliminate candidates revealed to be composite numbers by said small divisor test thereby yielding a sieved number of candidates (Page 145, Sec. 4.4.1);and performing at least one primality test on each said sieved number s of candidates (Page 148, Sec. 4.5.1)* [sic – 4.51], *each of the plurality s of primality tests including an associated exponentiation operation (Page 146, Sec. 4.4.1)."*

However, at Sec. 4.51, Menezes discusses a variation of a random search algorithm disclosed at Sec. 4.44, p.146:

> "1. Generate an odd *k*-bit integer *n* at random.
> 2. Use trial division to determine whether *n* is divisible by any odd prime < = *B* . . . .. If it is then go to step 1.
> 3. If MILLER-RABIN (*n,t*) (Algorithm 4.24) outputs "prime then return (*n*). Otherwise, go to step 1."

Thus, again, as in Sec. 4.1.1, candidates are selected one at a time, and primality testing is carried out on individual candidates in a sequential manner (note steps 1. and 3. above) by implementing the Sec. 4.44 algorithm. Menezes, in Sec. 4.51 discusses:

> "(i) An "alternative technique to generating candidates *n* at random in step 1 of Algorithm 4.44 is to first select a random *k*-bit odd number n_0, and then test the *s* numbers $n=n_0$, n_0+2, n_0+4, . . ., $n_0 + 2(s-1)$ for primality."

But this alternative does not change the underlying teaching of Menezes that primality testing is carried out in a sequential manner on individual candidates selected one at a time, which does not correspond to or suggest the recited features in claim 28:

> ". . . randomly generating a plurality of k random odd numbers expressed as $n_{0,0}$, $n_{1,0}$,... $n_{(k-1),0}$, each said number providing a prime number candidate; determining a plurality of y additional odd numbers based on each one of the randomly generated odd numbers $n_{1,0}$,... $n_{(k-1),0}$ to provide (k x y) additional prime number candidates ($n_{0,1}$, $n_{0,2}'$ ... $n_{0,y}$),

> $(n_{1,1}, n_{1,2}, \ldots n_{1,y}), \ldots(n_{(k-1),1}, n_{(k-1,)2}, \ldots n_{(k-1),y})$ thereby yielding a total number of (k x (y+1)) prime number candidates;"

Claim 29, dependent from claim 28, includes recitation of "successively adding two to each of said randomly generated odd numbers", and is differentiated from Menezes in a similar manner.

Nor does Menezes Sec. 4.51 disclose or suggest the parallel testing feature as recited in claim 28. This latter point, properly, is recognized by the Examiner:

> *"Menezes does not teach the exponentiation operations being executed by an associated one of a plurality of the exponentiation units . . ."*

In an attempt to remedy these deficiencies in Menezes, in the rejections of both claims 1 and 28, the Examiner relies on Qusiquater:

> *"Quisquater et al, teaches such a parallel arrangement of exponentiators (fig. 1, page 2 paragraph 7). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate these features into the method of Menezes. It would have been desirable to do so as this would allow for computation to proceed more rapidly. The motivation to make this combination is found for example, in Menezes Sec 4.1 Introduction where the efficiency of generation of public key parameters in public key systems such as RSA is discussed."*

[It is presumed the Examiner is citing to the paragraph headed *"Fast deciphering algorithm"* on the second page – believed to be page 906 – of the Quisquater reference.]

In the rejection of claim 1, the Examiner contends that Quisquater teaches a parallel arrangement of exponentiators but does not assert that Quisquater's exponentiators perform exponentiation operations "substantially simultaneously" and no reference to such operation is seen in Quisquater. However, this latter point is moot in the context of amended claims 1 and 28 neither of which recites the "substantially simultaneously" feature.

(In distinguishing Menezes, as noted above, the Examiner states: *"Menezes does not teach a processing system including a processing system including a processing unit and a plurality of exponentiation units communicatively coupled to the processing unit, . . ."*. The Examiner appears to make no assertion that these features are present in Quisquater and for these reason the stated grounds of rejection under 35 US 103 are incomplete.)

The Examiner's assertions related to Quisquater and Menezes are believed not to state a prima facie case of obviousness, as will be discussed below.

Under 35 USC 103, the burden of establishing a prima facie case of obviousness initially falls on the Examiner – MPEP 2142. Cited references must be considered in their entirety in relation to each other and in relation to the claim under rejection, considered as a whole. MPEP 2141.02. Accordingly, as set forth in MPEP 2142 and 2143, to establish a prima facie case, the Examiner must show that the references disclose or suggest all of the claimed elements. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, not in applicant's disclosure. *In re Vaeck,* 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).

Regarding motivation to combine, the Office Action states:

> *"[I]t would have been obvious to one of ordinary skill in the art . . . to incorporate these features [i.e. "a parallel arrangement of exponentiators" as disclosed with reference to Fig. 1] into the sequential testing method of Menezes. It would have been desirable to do so as this would allow for computation to proceed more rapidly. The motivation to make this combination is found for example, in Menezes Sec. 4.1 Introduction where the efficiency of generation of public key parameters in public key systems such as RSA is discussed."*

Menezes Sec. 4.1 Introduction, commences: "The efficient generation of public-key parameters is a prerequisite in public-key systems." The remainder of Section 4.1 outlines various such parameters rather than any particular way to effect "efficient generation" and thus does not comport with the Examiner's characterization. Such a sweepingly broad desideratum as "efficient generation" is so vague that it fails to provide any specific suggestion or motivation as to how Menezes might have been modified by Quisquater, let alone in a manner consistent with Menezes teaching of sequential testing of prime number candidates, one at a time. Neither Menezes nor Quisquater suggested desirability of or how to incorporate the teachings of Qusiquater into the methodology of Menezes. It is well established law that "[t]he mere fact that the prior art could be so modified would not have made the modification **obvious** unless the prior art suggested the **desirability** of the modification." *In re Gordon, 733* F.2d 900, *902, 221 U.S.P.Q. 1125* (Fed. Cir. *1984)* (emphasis added). As the Federal Circuit has stated, "virtually all [inventions] are combinations of old elements." *In re Rouffet, 149* F.3d *1350, 1357,*

47 U.S.P.Q.2d *1453* (Fed. Cir. *1998).* "Therefore an examiner may often find every element of a claimed invention in the prior art. If identification of each claimed element in the prior art were sufficient to negate patentability, very few patents would ever issue. Furthermore, rejecting patents solely by finding prior art corollaries for the claimed elements would permit an examiner to use the claimed invention itself as a blueprint for piecing together elements in the prior art to defeat the patentability of the claimed invention. Such an approach would be `an illogical and inappropriate process by which to determine patentability.'" *Id.*

These criteria show that the Examiner's theory of motivation lacks substance and is based on an improper hindsight consideration of the cited references. The Examiner is respectfully reminded that in applying 35 US 103, each cited reference each must be considered in its entirety -in relation to the claim under rejection considered as a whole – MPEP 2141.02.

Menezes and Quisquater do not individually or collectively disclose or suggest the whole combination of features set forth in claim 1 or claim 28. Menezes is not seen to disclose "generating a plurality of k random odd numbers each providing a prime number candidate" in conjunction with the primality testing features as recited in claim 1. To the contrary, in Menezes Sec. 4.1.1 (relied on by the Examiner), Menezes suggests as a "slight modification" to his basic scheme of generating and testing a particular random number (so that individual prime numbers are selected and tested sequentially), by using a particular search sequence (citing a search sequence n, n+2, n+4, n+6, . . .) to identify subsequent numbers to be tested individually. Thus, there is a known relationship between the subsequent numbers and the initial candidate number which does not equate with the above recitation in claim 1. Similarly, in Sec. 4.51 read in conjunction with Sec. 4.44, Menezes maintains this methodology of generating and testing an initial prime number candidate and then test further candidate numbers individually, each candidate having a defined relation with the initial number and this methodology clearly is different from and does not suggest the whole combination of features recited in claim 28, including: ". . . randomly generating a plurality of k random odd numbers expressed as $n_{0,0}$, $n_{1,0}$,... $n_{(k-1),0}$, . . . determining a plurality of y additional odd numbers based on each one of the randomly generated odd numbers $n_{1,0}$,... $n_{(k-1),0}$ to provide (k x y) additional

prime number candidates . . .thereby yielding a total number of (k x (y+1)) prime number candidates; . . .."

Quisquater, unlike Menezes whose teaching is directed to prime number generation, is directed to deciphering cryptograms - see title and abstract. In the passage cited by the Examiner, Quisquater teaches that "to decipher [a] cryptogram c, the algorithm first computes m^1 . . . and m^2 . . . rather than compute $m = c^d(\mathrm{mod}\, r)$ classically", and that "the two computations may be done in parallel." The Examiner has failed to provide any objective evidence that application of Quisquater's proposed implementation of his algorithm for deciphering a cryptogram would have any applicability in the context of Menezes technique for generating and testing prime number candidates in a sequential manner, as outlined by Menezes in Sec. 4.1.1. The assertion in the Office Action, "it would have been obvious to one of ordinary skill in the art . . . to incorporate these features [i.e. "a parallel arrangement of exponentiators" as disclosed with reference to Fig. 1] into the sequential testing method of Menezes" is unsubstantiated speculation. In fact, the Examiner's position amounts to arbitrary selection of an isolated feature from Quisquater (parallel arrangement of exponentiators) and a vague, general assertion ". . . it would have been obvious to incorporate these features into the method of Menezes", with no indication as to how the proposed incorporation might have been made attributable to any teaching or suggestion in either reference. The selective isolation from the context of Quisquater's cryptogram deciphering methodology of the "parallel computation" feature, and a speculative assertion of employment in an unspecified manner in Menezes system for sequential primality testing of individual prime number candidates, without regard to these different environments is untenable. It (a) fails to consider each reference in its entirety, (b) would have been inconsistent with Menezes sequential testing methodology of individual prime number candidates, contrary to the criteria in MPEP 2143.01 and (c) fails to teach the entire combination of features as recited in amended claim 1 or amended claim 28.

Nothing is seen in either reference that would have suggested in the context of claim 1:

> ". . . randomly generating a plurality of k random odd numbers each providing a prime number candidate; and performing a plurality of **t** primality tests on each of said plurality

> of k randomly generated prime number, each of the plurality of **(k x t)** primality tests including an associated exponentiation operation executed by an associated one of a plurality of **(k x t)** of the exponentiation units, said exponentiation operations being performed in parallel by said associated exponentiation units."

The final clause in claim 1 incorporates details of performance of primality tests on prime number candidates previously contained in claim 5 which was not rejected based on Menezes and Quisquater. Consequently, claim 1 is believed to be patentable over Menezes in view of Quisquater and in condition for allowance. Prior art rejections were not advanced against claims 2-11, directly or indirectly dependent from claim 1, which are also believed to be in condition for allowance as are dependent claims 12-14.

In the context of claim 28, nothing is seen in either reference that would have suggested the recited combination of features:

> ". . . randomly generating a plurality of k random odd numbers expressed as $n_{0,0}$, $n_{1,0}$,... $n_{(k-1),0}$, each said number providing a prime number candidate; determining a plurality of y additional odd numbers based on each one of the randomly generated odd numbers $n_{1,0}$,... $n_{(k-1),0}$ to provide (k x y) additional prime number candidates ($n_{0,1}$, $n_{0,2}$' ... $n_{0,y}$), ($n_{1,1}$, $n_{1,2}$, ... $n_{1,y}$), ...($n_{(k-1),1}$, $n_{(k-1,)2}$, ... $n_{(k-1),y}$) thereby yielding a total number of (k x (y+1)) prime number candidates; and performing at least one primality test on each of said sieved number s of candidates, each of the plurality of s primality tests including an associated exponentiation operation executed by an associated one of a plurality of s of the exponentiation units, said exponentiation operations being performed in parallel by said plurality of s exponentiation units in order to eliminate candidates revealed to be composite numbers by said primality test thereby yielding a remaining number r of candidates."

Prior art rejections were not advanced against claim 33 or claim 35 (dependent from claim 28) and those claims are believed to be in condition for allowance, as are dependent claims 29 and 34.

Claims 54 and 57 are rejected "on the same basis as claim 1" and the rejection is respectfully traversed. Claim 57, as originally presented, was similar in scope to original claim 5 which was not rejected over Menezes and Quisquater so that the rationale for rejection of claim 57 is unclear. The rejection is traversed in respect of amended claim 54 which, as amended, incorporates subject matter relating to primality testing recited in original claim 57. On that

basis, amended claim 54 should be allowable because Menezes and Quisquater do not render claim 54 obvious for similar reasons as those advanced above in respect of amended claim 1. Prior art rejections were not advanced against claims 55, 56 and 58-63, directly or indirectly dependent from claim 54, which are also believed to be in condition for allowance as is dependent claim 57, as amended.

CONCLUSION.

It is believed this amendment and response have addressed all grounds of rejection contained in the Office Action and has placed all pending claims in condition for allowance. Accordingly, favorable consideration and early allowance of the applications are respectfully solicited. If there are any remaining issues that could be resolved by discussion, a telephone call to the undersigned attorney at (972) 862-7428 would be appreciated.

Date: January 18, 2005
Hewlett-Packard Company
Intellectual Property Administration
3404 E. Harmony Road
Mail Stop 35
Fort Collins, CO 80528-9599

Respectfully submitted,

N. Rhys Merrett

N. Rhys Merrett
Attorney for Applicant
Reg. No. 27,250